Strengthening Cyber Resilience in Asia Pacific's Renewable Energy Sector

Snapshot

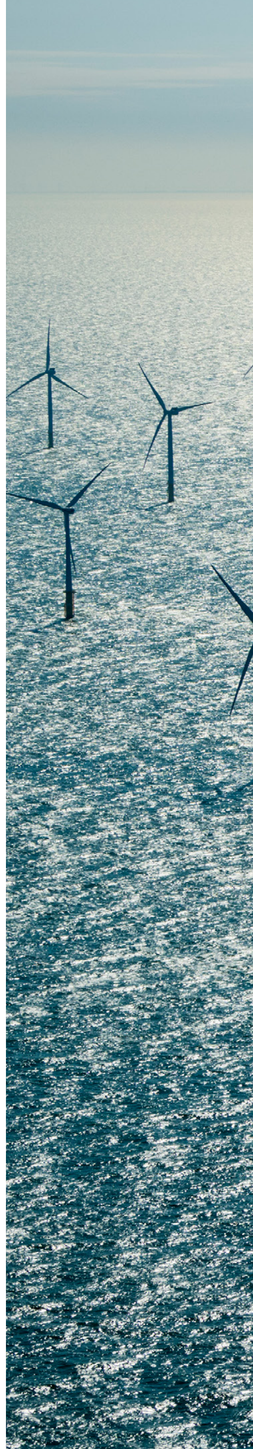
- The convergence of IT and operational technology (OT) systems in the renewables sector is increasing cyber risks.
- Both state-sponsored and financially motivated threat actors are intensifying attacks targeting critical infrastructure.
- While governments are strengthening cyber security frameworks, regulations remain inconsistent between countries and regions, potentially leaving critical energy systems exposed.
- Renewables companies must implement strong IT-OT segmentation, secure AI-driven systems, and leverage tailored risk transfer solutions in the ever-evolving threat landscape.

The renewable energy sector is at a pivotal moment. While global momentum continues to drive the transition to clean energy, skepticism and political uncertainty about renewables are creating new risks for the industry. Against this backdrop, the sector is also facing a growing threat from cyber-attacks targeting critical infrastructure. A successful cyber attack would not just disrupt energy production — it could become fuel for critics questioning the reliability of the energy transition as a whole.

Nowhere is this more relevant than in the Asia Pacific (APAC) region, where the shift to renewables is accelerating and cyber security threats are on the rise. In fact, incident frequency in APAC is up 29 percent year on year, and 134 percent over the past four years.[1] As the proportion of renewables on the grid grows, the potential impact of a cyber attack becomes greater, making the sector an increasingly attractive target. Geopolitical volatility is only amplifying the risk, as state-sponsored actors and cyber criminal groups are focusing their efforts on critical infrastructure, with Australia alone seeing 11% of reported cyber incidents last year affecting essential services like electricity and water.[2] The integration of smart grids with multi-directional flows of energy and data between renewable generators, batteries, and the grid has added efficiency and flexibility to energy systems, but has also rapidly expanded the attack surface.

While governments across APAC are strengthening their cyber security frameworks, regulatory measures remain inconsistent. Some countries, like Singapore[3] and Australia[4], have introduced stricter requirements on the renewables sector to protect critical infrastructure, while others have yet to establish comprehensive guidelines. This patchwork approach likely leaves gaps that threat actors can exploit, making it clear that regulation alone isn't enough.

Industry collaboration, real-time threat intelligence sharing, and innovative risk transfer strategies will be essential in ensuring cyber attacks do not undermine the credibility and stability of APAC's renewable energy future.



1. Aon analysis of Risk Based Security data, as of 25/03/2025
2. Reuters, Australia critical infrastructure faces cyber threats, 21 November 2024
3. Cyber Security Agency of Singapore, Cybersecurity Act, 2 April 2025
4. Cyber and Infrastructure Security Centre, Security of Critical Infrastructure Act 2018, April 2025

Cyber Risks on the Horizon

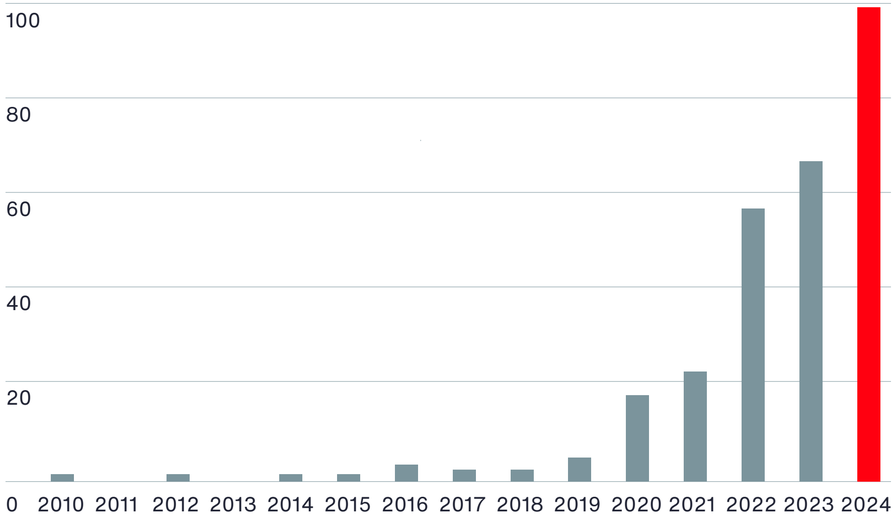
Cyber attacks on the energy sector have evolved beyond ransom-driven disruptions to more sophisticated exploits targeting operational technology (OT) systems.

Industrial control systems, such as SCADA and PLCs, used within the renewables sector for the delivery of services across wind and solar farms are increasingly being connected to IT systems or the cloud to achieve operational and maintenance efficiency. However, such technology often lacks secure-by-design features and is inherently difficult to patch for operational reasons and are thus increasingly vulnerable to attack.

In roughly one quarter of all cyber attacks with physical consequences since 2010, where public reports included enough detail, the threat actors impaired or manipulated OT systems directly, indicating a lack of adequate network segmentation.[5] In the remaining attacks, physical consequences were an indirect result of compromising IT systems or other kinds of systems upon which OT relies.

5. Waterfall Security, 2024 Threat Report – OT Cyberattacks with Physical Consequences, accessed February 2025

Global Count – Reported Cyber Attacks with Physical Consequences[6]



These risks are no longer theoretical. In 2024 in Japan, attackers hijacked approximately 800 SolarView Compact remote monitoring devices used in solar power facilities, exploiting a known vulnerability to install a backdoor.[7] While this breach was linked to financial fraud, it highlighted the ease and extent to which energy infrastructure could be compromised. Similar attacks on internet-connected solar inverters could manipulate energy outputs, destabilising the electric grid, or even causing physical damage to electronic systems.

The technology-driven renewable energy sector is particularly exposed: in 2024, unpatched vulnerabilities accounted for 49% of ransomware attack entry points.[8] For APAC's fast-growing renewables sector, these threats reinforce the urgent need for a proactive cyber resilience strategy. Organisations must prioritise patch management, strengthen endpoint security, and implement strict IT-OT segmentation to mitigate the growing risk of cyber-physical attacks and ensure the long-term stability of the energy transition.

> "Throughout the Asia Pacific region, renewable energy sources are increasingly meeting the electricity demands of growing economies. Given their rising strategic importance, vulnerabilities to cyber-attacks require constant vigilance, close collaboration, and comprehensive emergency response planning to ensure the resilience of energy supply."
>
> **Ben Waldron**
> Director, Power Engineering

6. Data extracted from Waterfall Security, 2024 Threat Report – OT Cyberattacks with Physical Consequences, accessed February 2025

7. IMC, Attackers hijack solar panel monitoring devices in Japan, 4 June 2024

8. Sophos, The State of Ransomware 2024, accessed February 2025

Supply Chain Vulnerabilities

Cyber threats to the renewables sector increasingly exploit weaknesses in the supply chain. Many wind farms and solar operations rely on original equipment manufacturers (OEMs) for ongoing monitoring and remote control of assets, creating potential entry points for attackers. Compromising a turbine OEM's system can provide hackers with access to multiple facilities across different operators, posing a serious risk to energy production and security.

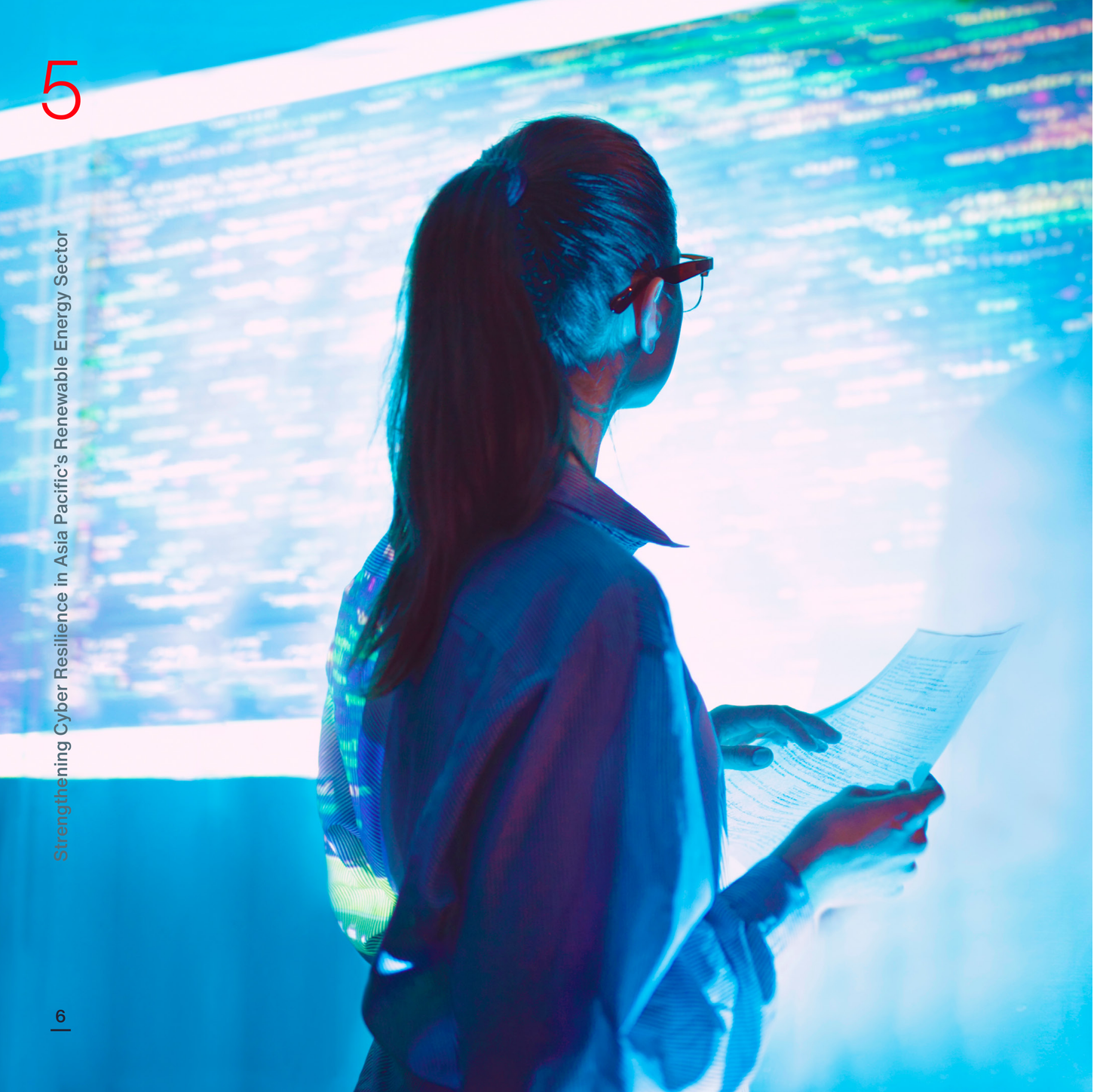
In 2022, a cyberattack on Enercon disrupted remote connectivity to nearly 6,000 wind turbines, preventing external monitoring and control, though the turbines continued operating in automatic mode.[9] Around the same time, German wind turbine manufacturer Nordex suffered a ransomware attack that forced the company to shut down remote access to protect its infrastructure.[10] Vestas, another leading wind turbine manufacturer, was also targeted in a ransomware attack, further exposing the sector's vulnerability to supply chain disruptions.[11]

- As supply chains become more interconnected, these incidents highlight how third-party systems can be leveraged to cause widespread operational disruptions.
- A large proportion of wind and solar technology entering APAC over the next decade is expected to come from Chinese manufacturers. While these suppliers have helped accelerate the clean energy transition, their involvement also raises complex cyber and geopolitical considerations — especially when it comes to remote access, firmware integrity, and data sovereignty. For critical infrastructure, risk managers should assess where systems are sourced and ensure procurement and vendor policies incorporate robust cyber security due diligence, access controls, and contingency planning.

9. Clean Energy Wire, Repeated cyberattacks cause concern about German wind industry's IT security, 24 May 2022

10. Nordex SE, Update on cyber security incident, April 2022

11. Vestas, Third update on cyber incident, December 2021



AI Challenges

While AI offers benefits to the renewables sector, including the ability to correlate large swathes of data across an industrial process to identify anomalies and potential attacks, it also introduces new cyber risks. Threat actors are leveraging AI to enhance cyber attacks, making spear phishing, whaling, and other social engineering tactics more sophisticated, and allowing the development of more advanced malware code at scale. Additionally, data poisoning — where attackers manipulate AI training data — could disrupt power supply models or compromise critical infrastructure.

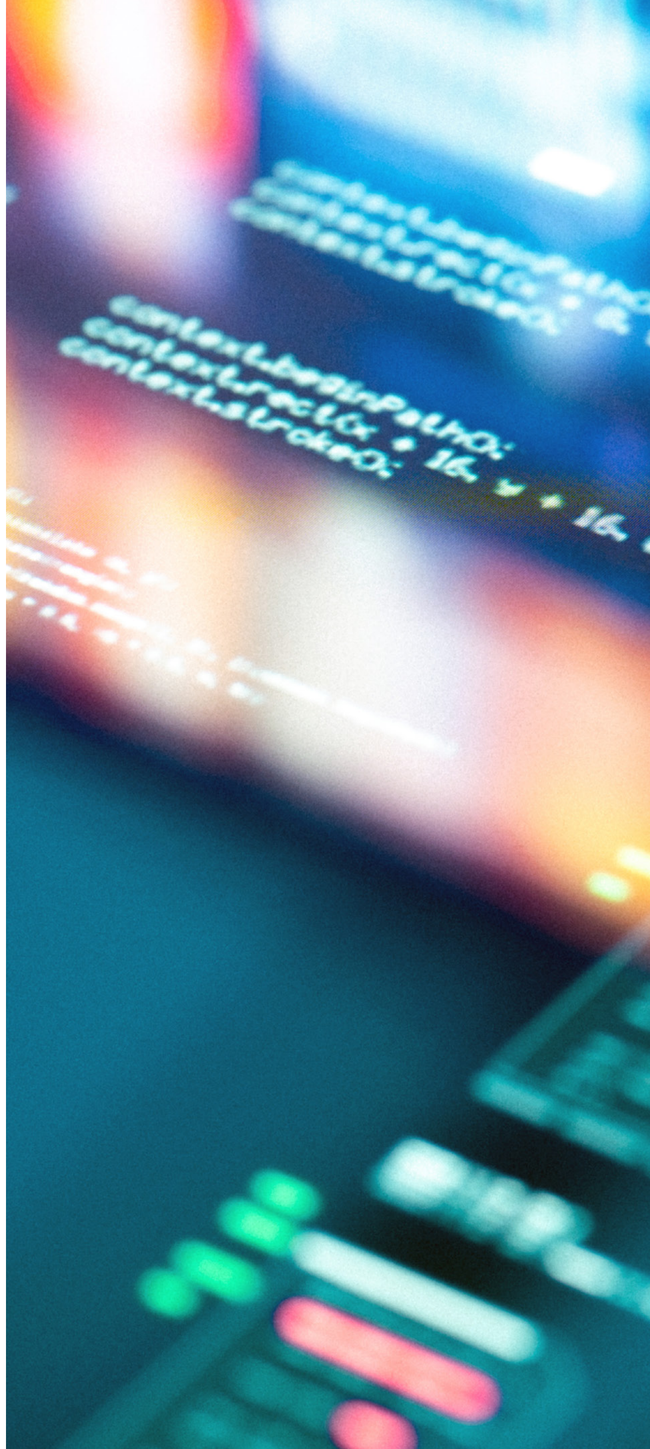
Another challenge is the rising electricity demand driven by AI adoption. More computing power means greater energy consumption, not just for processing but also for cooling data centres. In energy markets already facing supply and demand pressures, particularly in APAC's fast-growing economies, this additional strain could have broader implications for grid stability and resource allocation.

Building Cyber Resilience

Before renewable energy operators can effectively manage their cyber risk, they must first understand their exposure. A lack of visibility into potential attack surfaces leaves organisations vulnerable, making it difficult to prioritise cyber security investments or develop robust resilience strategies. Cyber risk quantification provides a structured, evidence-based approach to evaluating and measuring risk. By identifying the most relevant threats, companies can allocate resources more effectively and ensure cyber security discussions are aligned with broader business objectives. This approach also empowers CISOs to communicate the value of cybersecurity investments to senior leadership in a way that resonates with financial and operational decision-makers.

Despite growing awareness of cyber threats, the insurance market for renewables has yet to reach its full potential, partly due to uncertainties around catastrophe exposures and modelling. A significant protection gap remains. Expanding insurer participation will be key to strengthening coverage options for the sector.

> "Renewable energy operators need to contend with an increasingly complicated geopolitical climate and an ever-expanding cyber-attack surface. With threat actors increasingly seeking to target operational technology, the potential for physical damage to assets and resulting operational disruption has become amplified. Cyber risk transfer solutions are crucial to protect the financial and operational viability of renewable energy assets and can now more readily be expanded to address the cyber-physical damage coverage gap that has become commonplace under traditional insurance solutions."
>
> **Alex Eakins**
> Cyber Property Damage Practice Leader, Australia



Top Tips to Prepare for the Future of Cyber Risk in Renewables

To mitigate threats posed by the evolving cyber risk landscape, renewables organisations can:

- Build cyber resilience through a carefully planned strategy to manage cyber risk within the organisation. A lack of sufficient segmentation between IT and OT environments presents malicious actors with the opportunity to directly disrupt and damage industrial environments for energy companies through targeted cyber attacks.[12]
- Ensure that the incident response playbook and business continuity/disaster recovery plans have been assessed, reviewed and updated. Test them through simulated practice to help improve resilience.
- Use cyber scenarios to test worst-case outcomes from cyber attacks and identify existing vulnerabilities that can be addressed through risk management or transferred to an insurer. This is key for assets like those used in offshore wind, which rely on remote access systems to control wind farms that are a preferred target for threat actors.
- Assess core IT and OT environments and establish a security baseline or benchmark before extending to newly acquired assets and targeting control gaps. With cyber threats growing, special focus should be placed on endpoint system security. In 2023, approximately 70% of OT-related incidents originated from within the IT environment, whilst improperly configured firewalls were identified in 28% of client engagements over the same period.[13]
- Confirm that newly acquired assets have the same standard for cyber security as assets already in the portfolio. Aon has seen a sharp spike in loss activity following M&A activity in this industry due to insureds onboarding new assets without taking the appropriate measures to confirm cyber security measures are met.
- Monitor and adapt to new and evolving cyber security regulations, such as the Australian Security of Critical Infrastructure (SOCI) Act, which for critical electricity assets imposes mandatory notification timeframes for critical cyber incidents, as well as obligations in relation to the adoption, compliance and periodic review of risk management programs.
- Work with a risk advisor that can quantify potential financial, legal, reputational and property damage impacts from a cyber attack, map dependencies across critical assets and supply chains partners in your portfolio and overlay exposures with the insurance program to ensure it aligns with the materiality and complexity of the risk.
- Partner with a broker that can thoroughly review the exclusions within policies and address gaps in coverage.
- Strengthen supply chain and vendor management practices by ensuring third-party suppliers adhere to strict cybersecurity protocols. Many recent cyber incidents in the renewables sector have stemmed from vulnerabilities in vendor systems, such as turbine OEMs with remote monitoring and control access.

12. Dragos, 2023 OT Cybersecurity Year in Review, accessed February 2025
13. Dragos, 2023 OT Cybersecurity Year in Review, accessed February 2025

About Aon

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Through actionable analytic insight, globally integrated Risk Capital and Human Capital expertise, and locally relevant solutions, our colleagues provide clients in over 120 countries with the clarity and confidence to make better risk and people decisions that help protect and grow their businesses.

Follow Aon on LinkedIn, X, Facebook and Instagram. Stay up-to-date by visiting Aon's newsroom and sign up for news alerts here.

aon.com

Contact Us

Alex Eakins
Cyber Property Damage Practice Leader
alex.eakins@aon.com

Sabba Manyara
Director, Cyber Solutions, Asia
sabba.manyara@aon.com

Ben Waldron
Director, Power Engineering
ben.waldron@aon.com